International Journal of Computer Networking,
Wireless and Mobile Communications (IJCNWMC)
ISSN(P): 2250-1568; ISSN(E): 2278-9448
Vol. 4, Issue 2, Apr 2014, 83-92
© TJPRC Pvt. Ltd.

# MULTIPLE COOPERATIVE BLACK HOLE ATTACK DETECTION IN MOBILE AD HOC NETWORKS

**ROHINI SHARMA & MINAKSHI SHARMA**
Department of Computer Science, SSCET, Badhani, Punjab, India

## ABSTRACT

Mobile Ad-hoc network (MANET) is self configuring network also known as mesh network. It is a network of mobile devices connected by wireless links. Security is a major challenge for MANET because to their features of open medium, dynamically changing topologies, absence of centralized monitoring points. Thus, many routing protocols of MANETs are vulnerable to various types of attacks. Ad hoc on-demand distance vector routing (AODV) is a very popular routing protocol, vulnerable to the black hole attack, where a malicious node falsely advertises shortest and suitable paths to a destination node during the route discovery process.

This attack leads to severe stage if a group of malicious nodes cooperate each other. In this paper, a defense mechanism is proposed against multiple cooperative black hole nodes in a MANET. The simulation has been done that demonstrate the effectiveness of the mechanism in detection of the multiple malicious nodes while getting a better throughput and lesser delay in the network.

**KEYWORDS:** Mobile Ad Hoc Network (MANET), Blackhole Node, AODV Routing Protocol

## I. INTRODUCTION

An ad hoc network is a wireless network describe by the nonexistence of a centralized and fixed infrastructure. The absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks. Therefore, we refer to a wireless ad hoc network with mobile nodes as a Mobile Ad Hoc Network (MANET) [1]. Mobile Ad hoc network is a decentralized type of wireless network. There is no pre-existing infrastructure such as routers in wired networks or access points in wireless networks on which it is depended. In routing each node participates by forwarding data for other nodes in ad hoc network the determination of which nodes forward data is made dynamically on the basis of network connectivity. Mobile Ad-hoc networks are a new standard of wireless communication for mobile hosts. Basically it's a network which is used in urgent situation causes. No fixed infrastructure in ad hoc network like base stations is required. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. Wireless networks refer to those networks that make use of radio waves or microwaves in order to establish communication between the devices. All the nodes act as router in mobile ad hoc network [2].

MANET is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other and forming arbitrary topology. They can act as both routers and hosts. They have ability to self configure makes this technology suitable for provisioning communication to,

for example, disaster-hit areas where there is no communication infrastructure or in emergency search and rescue operations where a network connection is urgently required. In MANET routing protocols for both static and dynamic topology are used.

The Characteristics of MANETs have led to design of MANET specific routing protocols. There are mainly two types of routing protocol available Proactive (Table-driven) and Reactive (On- demand) Routing Protocol.

In recent years, a number of studies have been done on the different layers of the OSI Model, such as MAC layer and application, to achieve appropriate results. Our work focuses only on the routing/network layer. One of the most crucial problems of MANET is security of routing protocol. One of the most widely used routing protocols in MANETs is the ad hoc on-demand distance vector (AODV) routing protocol [3]. It is a source initiated on-demand routing protocol. However, AODV is vulnerable to the well-known black hole attack. In [4], the authors have proposed a solution to identify multiple black hole nodes cooperating as a group in an ad hoc network. The proposed technique works with slightly modified AODV protocol using Alarm Messages that is better than that technique with lesser delay and greater throughput.

The rest of the paper is organized as follows.

Section II discusses some related work in security mechanism in AODV routing protocol for MANETs. Section III gives an overview of AODV protocol and its security Problem. Section IV describes the proposed work on security. Section V presents the simulation results. Section VI concludes the paper while highlighting some future scope of work.

## II. RELATED WORK

The proposed work is aimed at developing better solution for AODV routing protocol against multiple cooperative black hole attack. As security problem has got attention of researchers. This section documents some of many techniques based on AODV developed by researchers.

Steven M. Bellov in and Michael Merritt et.al, discussed about Kerberos authentication protocol and various limitations of Kerberos authentication protocol [5]. The main limitation of Kerberos authentication protocol is much number of message exchange is needed for successful authentication and this approach will degrade the battery performance of the hand held devices. Second, disadvantage is the assumptions of the Kerberos authentication protocol when environment changes assumptions are need to change for efficient working of Kerberos protocol. Reply attack, login spoofing, session key expose, password guessing attacks are possible in Kerberos authentication protocol.

Seung Yi and Robin Kravets et.al had discussed various mutual authentication schemes of mobile ad hoc network. They had discussed the symmetric key and asymmetric key distribution schemes [6]. They had also discussed PKI (public key distribution) scheme which based on the symmetric key distribution scheme. In this paper author proposed a new authentication scheme named as MOCA which hybrid type of scheme and use both PKI and asymmetric schemes for mutual authentication. Pradeep kyasanur et.al proposed a protocol extension of 802.11 DCF protocol to detect the selfish behavior of the nodes in the infrastructure and ad hoc network topologies. Selfish nodes means the nodes which select the contentional window (CW) time in such a way so that the other nodes are keep on waiting to send the data and overall through put of the network degrade [7]. The proposed scheme has three components first one is that the receiver decides that whether sender is diverting form protocol or not. Second component is penalize ,in this scheme the receiver assigns the

contentional window time to the sender if sender not sends data in that time period sender have to pay the plenty. Plenty means that in next time when sender sends that data they have to wait more to send data to receiver. The third component is the diagnosis scheme receiver decide whether the sender is selfish or not on the basis of the total data send by the sender and number of times the sender pay plenty no of plenty paid by the sender is more than the threshold value which is fixed then the sender is selfish and no more data is received form that sender.

Tien-Ho Chen and Wei-Kuan Shih had discussed about importance of mutual authentication for wireless sensor networks .They also discussed about the DES protocol which is the hash-based authentication protocol [8]. This protocol provides the security against the stolen-verifier, masquerade, replay, and guessing attacks. In this paper they had also discussed about the weakness of the das protocol, they had proposed an certain enhancements in the das protocol. The enhanced das protocol is efficient than the traditional das protocol .Enhanced das protocol is reliable protocol and provides more security to the sensor nodes in the insecure environment. The proposed protocol is the energy efficient protocol and require less message exchange so as less traffic and less computations for mutual authentication.

Sushma Yalamanchi and K.V. Sambasiva Rao, they had proposed a two stage authentication scheme for wireless networks. They discus that in wired network use the authentication protocol which is having large computations but in wireless networks we require less computation and energy efficient authentication protocol. Because in wireless networks the hand held devices are having limited battery and limited computational resources also wireless networks on suffer from packet losses and bit errors and offers low bandwidth [9]. In the paper, they presents a two-stage authentication scheme for wireless networks that uses a computationally intensive but highly secure strong authentication in Stage 1 and a lightweight symmetric key based protocol in Stage 2. The cost of the strong authentication adopted in Stage 1 is amortized over N sessions thus reducing the overall cost of the scheme. They adapt the Dual-signature based IKE authentication that we proposed in our earlier work and employ it as Stage 1 authentication. The Symmetric key protocol in Stage 2 authentication that they proposed uses the symmetric keys that are generated in Stage 1. Priyanka Goyal et.al have introduced the elementary problems of ad hoc network by giving its background which is related to its work including the concept, status, features and vulnerabilities of MANET [10]. This paper presents summarized study of the routing protocols. Different types of Routing protocol like reactive, proactive and hybrid routing protocol and their subcategories all are mentioned in this paper. In the future how much bandwidth is required, how to scale up it and deployed it and which range of frequency is required all ways are explained. Also include the several challenging issues, emerging application like military battlefield, local level, Personal Area Network and the future trends of MANET. Karthikeyan U and Rajni introduced paper that challenge to study threats faced by the ad hoc network environment and provide an arrangement of the various security mechanisms [11]. The strengths and vulnerabilities of the existing routing protocols analyzed and suggest a broad and comprehensive framework that can provide a tangible solution. Hongmei Deng, Wei Li, and Dharma P. Agarwal [12] proposed the method for detecting the single black hole node. In this proposed method, each intermediate node sends back the next hop information when it sends back an RREP message. When the source node receives the reply message from intermediate node, it does not send the data packets quickly, but it extracts the next hop information and then sends the Further-Request to the next hop to verify that it has the route to the intermediate node. If the next hop has no route to the inquired intermediate node, but has a route to the destination node, we discard the reply packets from the inquired intermediate node, and use the new route through the next hop to the destination. At the same time, send out the alarm message to the whole network to isolate the malicious node. If the next hop has no route to the

requested intermediate node, and it also has no route to the destination node, the source node initiates another routing discovery process, and also sends out an alarm message to isolate the malicious node. One limitation of the proposed method is that it works based on an assumption that malicious nodes do not work as a group which is an unreal situation. Jaydip Sen, Sripad Koilakonda, Arijit Ukil [13] proposed a method for detecting multiple Cooperative Blackhole attacks. In the proposed scheme, two bits of additional information are sent by the nodes that respond to the RREQ message of a source node during route discovery process. Each node maintains an additional data routing information (DRI) table. In the DRI table, the bit 1 stands for 'true' and the bit 0 stands for 'false'. The first bit 'From' stands for the information on routing data packet from the node (in the Node filed), while the second bit 'Through' stands for information on routing data packet through the node (in the Node field). Another scheme relies on reliable nodes (nodes through which source has routed data previously and knows them to be trustworthy) to transfer data packets. Limitation of proposed method is that it detects only single cooperative attack with more delay and lesser throughput.

## III. AODV AND ITS SECURITY PROBLEMS

AODV protocol is written in RFC 3691. AODV is an important on-demand routing protocol that creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. It broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. In this process the intermediate node can reply to the RREQ packet only if it has a fresh enough route to the destination. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ. After selecting and establishing a route, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or the route is no longer desired. ARERR (Route Errors) message is used to notify other nodes that the loss of that link has occurred.

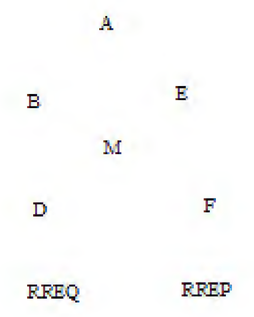


**Figure 1: Routing Discovery Process in AODV Protocol**

A black hole problem means that a malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. Imagine a malicious node 'M'. When node 'A' broadcasts a RREQ packet, nodes 'B' 'D' and 'M' receive it. Node 'M', being a malicious node, does not check up with its routing table for the requested route to node 'E'. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node 'A' receives the RREP from 'M' ahead of the RREP from 'B' and 'D'. Node 'A' assumes that the route through 'M' is the shortest route and sends any packet to the destination through it. When the node 'A' sends data to 'M', it absorbs all the data and thus behaves like a 'Black hole'.

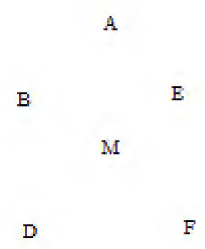


**Figure 2: Black Hole Attack in AODV Protocol**

In AODV, the sequence number is used to determine the freshness of routing information contained in the message from the originating node. When generating RREP message, a destination node compares its current sequence number, and the sequence number in the RREQ packet plus one, and then selects the larger one as RREPs sequence number. Upon receiving a number of RREP, the source node selects the one with greatest sequence number in order to construct a route. But, in the presence of black hole when a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from the other nodes. The source then starts to send out its packets to the black hole trusting that these packets will reach the destination. Thus the black hole will attract all the packets from the source and instead of forwarding those packets to the destination it will simply discard those. Thus the packets attracted by the black hole node will not reach the destination.

## IV. THE PROPOSED WORK

The proposed mechanism uses the fake RREQ message to attract the malicious node to respond the fake RREP message. In our scenario, there is more than one malicious node who will reply the fake RREQ packet.

- In this mechanism, before discovering the actual route for data transmission in AODV, a fake RREQ packet is broadcasted which includes the target or destination address which does not exist in reality.
- The multiple black hole nodes will immediately respond to the fake RREQ packet as they do not care about whether the fake target addressed node exists or not in the network. Then, the RREP packet will be sent by those multiple black hole nodes.
- The RREP packet is here enhanced by adding one more field as Record Field using the reserved bits of RREP packet. This field is used to contain the information about the identity of the node who replies the RREP packet to the source node. When any node in the network reply RREP packet, its identity will be recorded into Record field. So, if any intermediate node sends the RREP packet in response to the fake RREQ, it can be easily traced or detected.

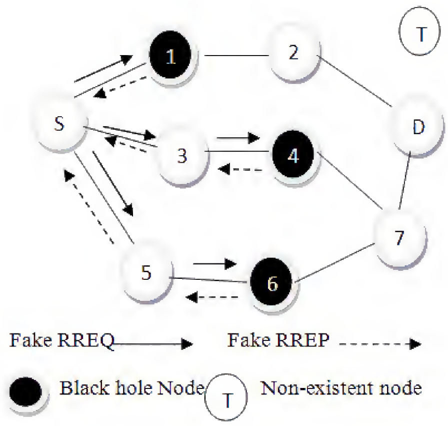


**Figure 3: Sending Fake RREQ Packet**

In figure 3, we have three black hole nodes located at different places in the network named as 1, 4 and 6. Before the initiating the actual route discovery process in AODV, the source node broadcast the fake RREQ message with fake target address of node T (non-existent node) to the neighboring nodes 1, 3 and 5.

- The normal nodes having no malicious behavior will not reply to the fake RREQ message as they have no route to that virtual node T. The malicious nodes 1, 4 and 6 will reply the RREP packet as advertising the shortest path towards the destination node (T).
- The identity of these nodes will be recorded into the Record field of the RREP packet. When the source node S receives the multiple RREP packets, from the Record field it will be able to trace the identity of malicious nodes.
- These identities will be added to the black list and this list will be broadcast as an ALARM packet to all the nodes in the network. Then, these multiple black hole nodes will be isolated from the network. After isolating the multiple black hole nodes, the normal route discovery process in AODV will be initiated. The data is then routed to the destination.
- If the packet delivery ratio is down to some threshold value that has been decided on the basis of average packet delivery ratio (threshold value).
- Also, the end to end delay is checked if it is more than the average end to end delay of data packets, then there will be chances of attack.
- The threshold values for packet delivery ratio and end to end delay is taken as the average of normal PDR and end to end delay of data packets respectively.
- Normal Operation of AODV.
- If(packet delivery ratio<threshold_value1 and end to end delay>threshold_value2)
- Then, again the source node will restart the process of broadcasting fake RREQ packet to detect the single or multiple black hole nodes.

The detection of single or multiple black hole nodes have done early before initializing the route discovery process in AODV. It makes this method more effective. After the detection process, there is an additional check to find out

the packets are again dropped or not during normal transmission of data packets after normal route discovery process. This additional check is calculating the packet delivery ratio, if it comes down to some threshold value (average PDR). And also, if end to end delay, the time taken for the data packets to transfer from source to destination, is more as compare to the average end to end delay of data packets (threshold_value2). Then, there is the maximum chance of existence of blackhole nodes. Again, the detection mechanism will be started.

## V. SIMULATIONS

The experiments for the evaluation of the proposed scheme have been carried out using the network simulator ns-2.

**Table 1: Simulation Parameters**

| Parameter | Value |
|---|---|
| Simulation Duration | 1200 sec |
| Simulation area | 800x800 |
| Number of mobile nodes | 20 |
| Transmission range | 200 m |
| Movement model | Random waypoint |
| Maximum speed | 5 – 20 m /sec |
| Traffic type | CBR (UDP) |
| Total number of flows | 12 |
| Packet rate | 2 packets / sec |
| Data payload | 512 bytes / packet |
| Number of malicious nodes | 2 |
| Host pause time | 5 sec |

Following metrics are chosen to evaluate the impact of the black hole attack on the simulated network: (i) Throughput and (ii) Delay.

In Figure 4 Average End to End delay vs. numbers of nodes for both old and new scenario is represented. Green line represents the delay in the new scenario and red line represents the delay in old scenario. Due to black hole attack in the network the delay in the old scenario increase with steady rate as compared in the new scenario.

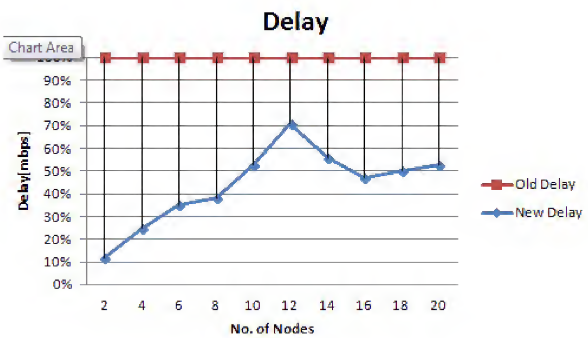


**Figure 4: Average End to End Delay vs. Numbers of Nodes**

In Figure 5 Packet Delivery Ratio vs. numbers of nodes for both old and new scenario is represented. Green line represents the throughput in the new scenario and red line represents the throughput in old scenario. Due to black hole attack in the network the throughput in the old scenario decrease with steady rate as compared in the new scenario.

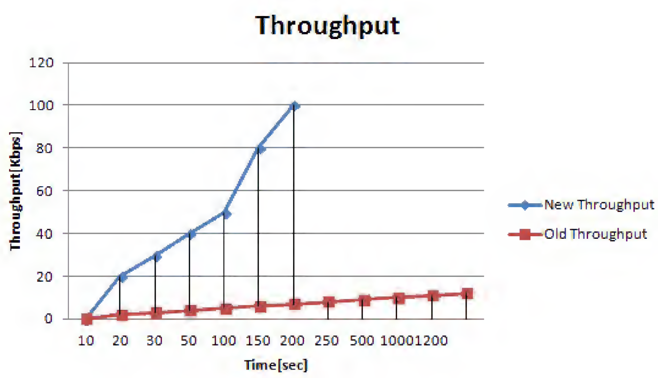


**Figure 5: Packet Delivery Ratio vs. Numbers of Nodes**

## VI. CONCLUSIONS

In this paper, Security issue in MANETs is presented. The Multiple cooperative blackhole attack in AODV has also been described. A better solution has been proposed to identify multiple blackhole nodes in a MANET to identify a secure routing path from a source node to a destination node. The proposed mechanism has been implemented in the network simulator *ns-2*, and the results or graphs demonstrate the effectiveness of the mechanism. In future the proposed security mechanism may also be extended by defending against grayhole attack- an attack where some nodes switch their states from blackhole to honest intermittently and vice versa, is also an interesting future work.

## VII. REFERENCES

1. Giovanni Vigna Sumit Gwalani Kavitha Srinivasan Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool for AODV-based Ad-hoc Wireless Networks*", 2004.*

2. Abdul Haimid Bashir Mohamed, Thesis, "Analysis and Simulation of Wireless Ad-hoc Network Routing Protocols"*2004.*

3. Annapurna P.Patil, Dr K Rajani Kanth et.al, "Design of an Energy Efficient Routing Protocol for MANETs based AODV", *IJCSI, Vol. 8, No.1, July 2011.*

4. H. Deng, H. Li, and D. Agrawal, "Routing security in wireless ad hoc networks", *IEEE Communications*

5. *Magazine, Vol. 40, No. 10, Oct 2002.*

6. Steven M. Bellovin and Michael Merritt "Limitations of the Kerberos Authentication", *USENIX – winter 1991.* [6] Seung Yi, Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks", *10 th IEEE International Conference on Network Protocols (ICNP'02)1092-1648.*

7. Pradeep kyasanur, "Selfish MAC layer Misbehavior in wireless networks", IEEE on Mobile Computing, 2005.

8. Tien-Ho Chen and Wei-Kuan, Shih, "A Robust Mutual Authentication Protocol for Wireless Sensor Networks", *ETRI Journal, Volume 32, Number 5, October 2010.*

9. Sushma Yalamanchi and K.V. Sambasiva Rao "Two-Stage authentication for wireless networks using dual signature and symmetric key protocol" *International Journal of Computer Science and Communication (IJCSC), Vol. 2, No. 2, July-December 2011, pp. 419-422.*

10. Priyanka goyal, vinit, Rishi, "MANET- A vulnerable, challenge, attacks and application*", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.*

11. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", *Springer 2006.*

12. Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network*", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.*

13. Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", *Second International Conference on Intelligent Systems, Modeling and Simulation,2011.*


## APPENDICES

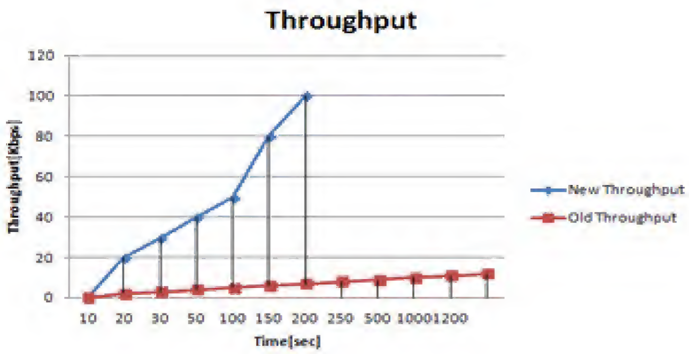


**Figure 6**

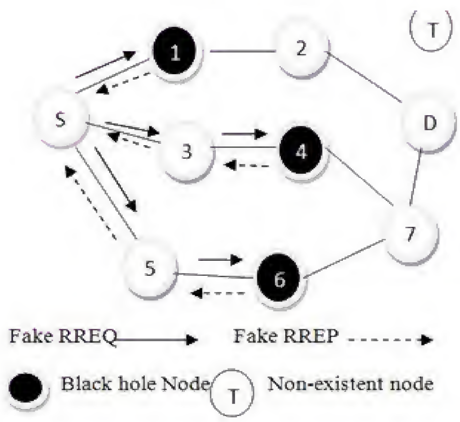


**Figure 7**

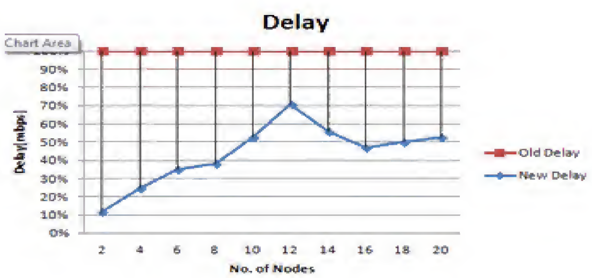


**Figure 8**

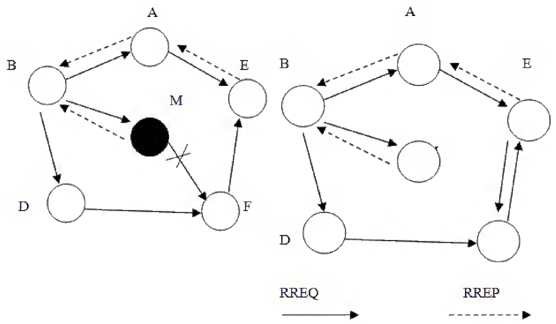


**Figure 9**

**Table 2: Simulation Parameters**

| Parameter | Value |
|---|---|
| Simulation Duration | 1200 sec |
| Simulation area | 800x800 |
| Number of mobile nodes | 20 |
| Transmission range | 200 m |
| Movement model | Random waypoint |
| Maximum speed | 5 – 20 m /sec |
| Traffic type | CBR (UDP) |
| Total number of flows | 12 |
| Packet rate | 2 packets / sec |
| Data payload | 512 bytes / packet |
| Number of malicious nodes | 2 |
| Host pause time | 5 sec |